

## REMARKS

As a preliminary note, although the pending claims have not been formally rejected, Applicants wish to point out that among other things, the black list described in the Perlman reference and the operation of the user's computer in Perlman et al. is distinctly different from Applicants' claimed invention. For example, Perlman et al. appears to be silent as to, among other things, that the end user provides certificate update subscription information that includes the identity of a plurality of subscriber subjects that the end user is interested in communicating with to effectively allow selective update information for a subscriber subject selected by an end user. Moreover, the claims require, among other things, providing the certificate update subscription information to the server to allow the server to selectively provide update information for those subscriber subjects selected by the end user. In contrast, the blacklist of Perlman et al. is simply a list of only revoked or invalid certificates none of which appear to be selectively chosen by the end user nor selectively evaluated by the server. The blacklist does not include expired certificates in order to reduce bandwidth. The certification authority of Perlman et al. issues a list of certificates that have been revoked either periodically or on demand containing a list of certificates that have been issued in the past but which are now to be considered invalid. The blacklist supplements lists that include expired certificates. Accordingly, Perlman et al. does not, among other things, monitor a specific public key certificate in response to subscription information or notifying a user when it changes. In fact, it appears that the user merely stores the blacklist as sent by the server, and does not update, select or provide update subscription information. Accordingly, the claims are believed to be in condition for allowance.

Attached hereto is a marked up version of the changes made to the claims by the current amendment,. The attached page is captioned "Version With Markings to Show Changes Made."

[illegible]

By: Christopher J. Reckamp  
Christopher J. Reckamp  
Registration No. 34,414

VEDDER, PRICE, KAUFMAN &  
KAMMHOLZ  
222 N. LaSalle Street  
Chicago, IL 60601  
(312) 609-7500  
FAX: (312) 609-5005

**VERSION WITH MARKINGS TO SHOW CHANGES MADE**

8. (Once Amended) A method for providing certificate updates, the method comprises the steps of:

a) [from time to time, receiving a public key certificate update subscription information from a user, wherein the public key certificate update subscription information identifies at least one subscriber subject and a public key of the at least one subscriber subject]generating, by an end user, certificate update subscription information that includes at least identity of a plurality of subscriber subjects that the end user is interested in and their associated public keys, and receiving the certificate update subscription information from the user, wherein the certificate update subscription information includes current certificates for those subscriber subjects that the end user has a desire to communicate with, at least one of identity of at least one of subscriber subject, a public key certificate of the at least one subscriber subject, an attribute certificate of the subscriber subject, identity of a certification authority and a cross-certificate;

b) monitoring certificate of the at least one subscriber subject; [and]

c) when a change occurs to the [public key]certificate, providing an indication of the change to the user[.];

the method further comprising receiving an indication of a user replica of the certificate from the user, when the use is on-line;

determining whether the user replica of the certificate is consistent with server replica of the certificate; and

when the user replica of the certificate is inconsistent with the server replica of the certificate, providing an indication of the server replica of the certificate to the user.

15. (Once Amended) A method for obtaining public key certificate updates, the method comprising the steps of:

a) [from time to time, providing, by a user, public key certificate subscription to a server, wherein the public key certificate update subscription information identifies at least one

subscriber subject and a public key of the at least one subscriber subject]generating by a user, certificate update subscription information that includes at least identity of at least one subscriber subject that the end user is interested in and their associated public keys, and providing y the user, the public key certificate update subscription information to a server, wherein the public key certificate update subscription information identifies at least one subscriber subject that the end user is interested in and their associated public keys;

- b) monitoring, by the server, public key certificate of the at least one subscriber subject;
- c) when a change occurs to the public key certificate, providing by the server, an indication of the change to the user;
- d) while on-line, receiving, by the user, the indication of the change; and
- e) determining, by the user, newly updated public key certificate based on the indication of the change.

24. (Once Amended) A server of secure communication system, wherein the server comprises:

processing unit; [and]

memory operably coupled to the processing unit, wherein the memory stores programming instructions that, when read by the processing unit, causes the processing unit to (a) [from time to time, receive a public key certificate update subscription information from a user, wherein the public key certificate update subscription information identifies at least one subscriber subject and a public key of the at least one subscriber subject]generate by a user certificate update subscription information that includes at least identity of at least one subscriber subject that the end user is interested in and their associated public keys, and receive the certificate update subscription information from the user, wherein the certificate update subscription information for those subscriber subjects that the end-user has a desire to communicate with includes at least one of: identity of at least one of subscriber subject, a public key certificate of the at least one subscriber subject, an attribute certificate of the subscriber

subject, identity of a certification authority and a cross-certificate; (b) monitor [public key] certificate of the at least one subscriber subject and the certification authority; [and](c) provide an indication of a change to the user when the change occurs to the [public key] certificate; and

(i) receive an indication of a user replica of the certificate from the user, when the user is on-line; (ii) determine whether the user replica of the certificate is consistent with server replica of the certificate; and (iii) provide an indication of the server replica of the certificate to the use when the user replica of the certificate is inconsistent with the server replica of the certificate.

FOIA b 7 - E 340001